NOTICE

U.S. Department of Transportation
Federal Aviation Administration

N 8110.91

01/16/01

Cancellation Date: 01/16/02

SUBJ: GUIDELINES FOR THE QUALIFICATION OF SOFTWARE TOOLS USING RTCA/DO-178B

1. PURPOSE. This notice provides guidelines to Aircraft Certification Office (ACO) engineers and to Designated Engineering Representatives (DER) regarding the application of RTCA/ DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," to the qualification of software verification and development tools. Advisory Circular (AC) 20-115B, "RTCA, Inc. Document RTCA/DO-178B," recognizes DO-178B as an acceptable means of compliance for securing the FAA's approval of software in airborne systems and equipment. Section 12.2 of DO-178B addresses tool qualification; however, the Section 12.2 criteria are often misinterpreted and result in inconsistent application in the field. This notice clarifies the application of DO-178B in the area of tool qualification but does not change the intent of DO-178B in this area. The guidelines in this notice should be used in applying the criteria in DO-178B for the qualification of tools.

2. DISTRIBUTION. This notice is distributed to the branch level in Washington Headquarters Aircraft Certification Service, section level in all Aircraft Certification Directorates, all National Resource Specialists (NRS), all Aircraft Certification Offices (ACO), all Manufacturing Inspection Offices (MIO), all Manufacturing Inspection District or Satellite Offices (MIDO/MISO), and all Flight Standards District Offices (FSDO). Additional limited distribution should be made to the Air Carrier District Offices, the Aeronautical Quality Assurance Field Offices, and the FAA Academy.

3. RELATED PUBLICATIONS.

a. Advisory Circular 20-115B, "RTCA, Inc. Document RTCA/DO-178B," dated January 11, 1993.

b. RTCA, Incorporated, document RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," dated December 1, 1992.

4. BACKGROUND. On January 11, 1993, the FAA issued AC 20-115B, which recognizes DO-178B as a means of demonstrating compliance to the regulations for the software aspects of airborne systems and equipment. Section 12.2 of DO-178B states that qualification of a tool is needed when processes in DO-178B "are eliminated, reduced, or automated by the use of a software tool, without its output being verified as specified in section 6" of DO-178B. DO-178B states, "The objective of the tool qualification process is to ensure that the tool provides confidence at least equivalent to that of the process(es) eliminated, reduced, or automated." The items below provide further information regarding tool qualification:

a. Software development can be a very repetitive and human-labor intensive process. This can result in errors, as well as high costs. For these reasons various tools have been developed to automate portions of this process. If the tools are dependable, then improvements in productivity and lower numbers of in-service errors may be realized.

b. In order to certify systems developed by tools, the FAA, DER's, and applicants need to obtain confidence by qualification that these tools are dependable. DO-178B Section 12.2 was designed to provide criteria for establishing which tools require additional confidence and the criteria and data needed to establish that confidence. However, a number of provisions of this section are difficult to interpret. This notice provides a means to clarify the intent of DO-178B Section 12.2 and its application.

c. Some areas that have resulted in misinterpretation and inconsistent application of the DO-178B tool qualification criteria are:

(1) When a tool should be qualified.

(2) Justification for the different criteria for qualifying software development tools and software verification tools.

(3) Which criteria apply to software development tools and which apply to software verification tools.

(4) Data to be produced for software development tools and for software verification tools.

(5) Acceptance criteria for tool operational requirements.

(6) Tool determinism.

(7) Tool partitioning assurance and evidence.

(8) Tool configuration control.

d. These areas have resulted in inconsistencies in applying the criteria within DO-178B Section 12.2 to certification projects. This notice is designed to address the above problems by clarifying the intent and application of DO-178B Section 12.2.

5. DISCUSSION.

a. Not all software tools require qualification. According to DO-178B Section 12.2, qualification of a tool is needed only when processes described in DO-178B are eliminated, reduced, or automated by the use of that tool without its output being verified as specified in DO-178B Section 6. This means that if the results of the tool are being relied on to supply the sole evidence that one or more objectives are satisfied, the tool is required to be qualified per DO-178B Section 12.2. If the output of the tool is verified by some other means, then there is no need to qualify the tool. For example, if all the outputs of a test case generator are reviewed to ensure that coverage is achieved, then the tool does not need to be qualified. This notice provides guidelines to determine whether a particular tool requires qualification.

b. DO-178B Section 12.2 identifies two types of tools: software verification tools and software development tools. Each type will be discussed below.

c. DO-178B defines verification tools as "tools that cannot introduce errors, but may fail to detect them."

(1) The following are examples of verification tools:

(a) A tool that automates the comparison of various software products (e.g., code, design) against some standard(s) for that product.

(b) A tool that generates test procedures and cases from the requirements.

(c) A tool that automatically runs the tests and determines pass/fail status.

(d) A tool that tracks the test process and reports if the desired structural coverage has been achieved.

(2) Many claim that verification tools can be more reliable than humans in a number of verification tasks, if their correct operation is demonstrated. In order to encourage the use of verification tools, DO-178B Section 12.2 was designed to provide an acceptable approach to qualifying verification tools.

d. DO-178B defines development tools as “tools whose output is part of airborne software and thus can introduce errors.” If there is a possibility that a tool can generate an error in the airborne software that would not be detected, then the tool cannot be treated as a verification tool. An example of this would be a tool that instrumented the code for testing and then removed the instrumentation code after the tests were completed. If there was no further verification of the tool’s output, then this tool could have altered the original code in some unknown way. Typically, the original code prior to instrumentation is what is used in the product. This example is included to demonstrate that tools used during verification are not necessarily verification tools. The effect on the final product must be assessed to determine the tool’s classification.

e. The reason for the distinction between development and verification tools is based on the likelihood of allowing an error into the airborne system. For development tools there is a potential to introduce errors directly into a system. However, a verification tool can only fail to detect an error that already exists in the product; therefore, a verification tool would need to be deficient in two different processes to allow an error to get into the airborne software: the development process introducing the error and the verification process to detect the error. For this reason, DO-178B calls for different levels of rigor in the qualification of verification and development tools.

6. PROCEDURES. For any project involving the qualification of tools, the ACO engineer and/or DER (if authorized) should follow the procedures and guidelines listed in this section:

a. Guidelines for determining whether a tool should be qualified:

(1) Whether a tool needs to be qualified is independent of the type of the tool (development or verification). There are three questions to ask to determine if a tool needs qualification. If the answer is "Yes" to all of the questions below, the tool should be qualified:

(a) Can the tool insert an error into the airborne software or fail to detect an existing error in the software within the scope of its intended usage?

(b) Will the tool's output not be verified as specified in Section 6 of DO-178B?

(c) Are processes of DO-178B eliminated, reduced, or automated by the use of the tool? That is, will the output from the tool be used to either meet an objective or replace an objective of DO-178B, Annex A?

(2) Once it has been determined that a tool does not require qualification, the remainder of DO-178B Section 12.2 is not applicable to that tool. In order to ensure timely response, the cognizant ACO engineer or DER (if authorized) should be involved early in the certification project's tool qualification agreements.

(3) The Plan for Software Aspects of Certification (PSAC) should include a listing of all software tools and justification for why each tool does or does not require qualification.

b. Guidelines for determining which tool qualification criteria apply to development tools and which criteria apply to verification tools:

(1) Table 1 applies to tools requiring qualification and can be used to determine which criteria of DO-178B Section 12.2 apply to which type of tool. Table 1 shows the similarities and differences in the qualification criteria for development and verification tools. The column in Table 1 titled "Criteria" summarizes the DO-178B requirement; the column titled "Dev./Ref." lists the applicability of the criteria for development tools and the appropriate DO-178B section

reference; and the column titled "Verif./Ref." lists the applicability of the criteria for verification tools with the appropriate DO-178B section reference.

Table 1 – DO-178B Criteria Applicable to Tool Qualification

Criteria	Dev./Ref.	Verif./Ref.
Only deterministic tools may be qualified (to be further clarified in Section 6f of this notice).	Yes/12.2	Yes/12.2
Qualification should only be for a specific system; the intention should be stated in the PSAC.	Yes/12.2	Yes/12.2
Combined tools should be qualified to DO-178B, Section 12.2.1 unless partitioning can be shown (to be further clarified in Section 6g of this notice).	Yes/12.2.b	Yes/12.2.b
Software configuration management and software quality assurance process objectives should be applied to tools being qualified (to be further discussed in Section 6h of this notice).	Yes/12.2.c	Yes/12.2.c
Qualification should satisfy the same objectives as the airborne software.	Yes/12.2.1.a	No
The software level of the tool may be reduced.	Yes/12.2.1.b	No
A trial period may be used as a means of qualification.	Yes/ 12.2.1.c	Yes/12.2.2
Tool Operational Requirements should be reviewed.	Yes/12.2.1.d(1)	Yes/12.2.2
Compliance with Tool Operational Requirements under normal operating conditions should be demonstrated.	Yes/12.2.1.d(2)	Yes/12.2.2
Compliance with Tool Operational Requirements under abnormal operating conditions should be demonstrated.	Yes/12.2.1.d(3)	No
Requirements-based coverage should be analyzed.	Yes/12.2.1.d(4)	No
Structural coverage appropriate for the tool's software level should be completed.	Yes/12.2.1.d(5)	No
Robustness testing appropriate for the tool's software level should be completed.	Yes/12.2.1.d(6)	No
Potential errors should be analyzed.	Yes/12.2.1.d(7)	No

c. Guidelines for data submittal and data availability to demonstrate tool qualification. The requirements for data to support tool qualification are listed throughout DO-178B Section 12.2; however, there is no definitive guidance as to the minimum level/amount of data to be submitted to the FAA for tool qualification. The data submittals vary according to the type of tool being developed. Even though there are some similar requirements for the two tool types, the data requirements for each tool type are different. Table 2 summarizes the required tool qualification data. The column titled "Data" lists the required data for tool qualification. The column titled "Applicability" summarizes if the data is applicable for development tool qualification (Development) or verification tool qualification (Verification). The column titled "Available/Submit" summarizes if the data should be submitted to the FAA or just available for FAA review. The column titled "DO-178B Ref." lists the DO-178B section reference to the criteria. The remainder of this section discusses the tool qualification data summarized in Table 2.

Table 2 – Data Required for Tool Qualification

Data	Applicability	Available/ Submit	DO-178B Ref.
Plan for Software Aspects of Certification (PSAC)	Verification & Development (see Note 1 below)	Submit	12.2, 12.2.3.a, & 12.2.4
Tool Qualification Plan	Development Only (see Note 2 below)	Submit	12.2.3.a(1), 12.2.3.1, & 12.2.4
Tool Operational Requirements	Verification & Development	Available	12.2.3.c(2) & 12.2.3.2
Software Accomplishment Summary (SAS)	Verification & Development (see Note 1 below)	Submit	12.2.4
Tool Qualification Accomplishment Summary	Development Only (see Note 2 below)	Submit	12.2.3.c(3) & 12.2.4
Tool Verification Results	Verification & Development	Available	12.2.3.c
Tool Qualification Development data (e.g., design, code, test cases and procedures)	Development Only	Available	12.2.3.c

NOTE 1: For development tool qualification, the PSAC should reference the Tool Qualification Plan and the SAS should reference the Tool Qualification Accomplishment Summary.

NOTE 2: The Tool Qualification Plan and the Tool Qualification Accomplishment Summary may be developed for verification tool qualification, if the applicant so desires.

(1) Verification Tool Qualification Data. Of the two tool qualification types, verification tools require the fewest data submittals and availability. Data for verification tool qualification are discussed below:

(a) For verification tools, the applicant should specify the intent to use a verification tool in the PSAC (reference DO-178B, Section 12.2). The PSAC should be submitted to the FAA. This alerts the ACO engineer to provide a response to the intended use of the tool and opens a dialogue on acceptable qualification methods and documentation approaches. The ACO engineer and/or DER (if authorized) should provide written response to the applicant on the acceptability of the approach listed or referenced in the PSAC in a timely manner (i.e., the verification tool qualification approaches in the PSAC should be reviewed and approved or addressed in a timely manner).

(b) For verification tool qualification, the Tool Operational Requirements should be documented and available to the FAA (reference DO-178B, Section 12.2.3.2). The requirements for the Tool Operational Requirements data are discussed in Section 6d of this notice.

(c) Data that shows that all of the requirements in the Tool Operational Requirements have been verified should also be documented and available for FAA review. Sufficient verification data is needed to demonstrate normal operation only and will vary depending on the complexity of the tool, the purpose of the tool, and how the tool is used. This verification data may be packaged in any document deemed acceptable by the applicant.

(d) An entry summarizing the results of the verification tool qualification should be included in the Software Accomplishment Summary (SAS). The SAS should be submitted to the FAA. This allows the ACO engineer to approve the results of the verification data and is evidence of the tool's qualification status.

> NOTE: The applicant may choose to provide a separate Tool Qualification Plan and Tool Accomplishment Summary referenced by entries in the PSAC and the SAS for software verification tools. Entries are still required in the PSAC and SAS. This is an acceptable approach with the added benefit of providing the ability to reference a data package for reuse in subsequent certifications or in different certifications where the usage of the tool can be shown to be identical.

(2) Development Tool Qualification Data. There are additional requirements for a software development tool. The development tool data is similar to the requirements for the airborne software application development. For the software development tool qualification, the following data submittal and availability items should be considered:

(a) For the development tool qualification, the actual qualification approach and data to be provided are specified in the Tool Qualification Plan. The Tool Qualification Plan should be submitted to and approved by the FAA.

(b) The Tool Qualification Accomplishment Summary is also required for development tool qualification. It summarizes the results of the tool qualification process and describes and references the relevant tool qualification data. It should be submitted to and approved by the FAA.

(c) For development tool qualification, the PSAC and SAS should be submitted to and approved by the FAA. However, these documents will likely only reference the Tool Qualification Plan and the Tool Qualification Accomplishment Summary documents.

(d) For development tool qualification, the Tool Operational Requirements should be documented and available to the FAA (reference DO-178B, Section 12.2.3.2). The requirements for the Tool Operational Requirements data are discussed in Section 6d of this notice.

(e) Data that shows that all of the requirements in the Tool Operational Requirements have been verified should also be documented and made available for FAA review. Sufficient verification data is needed to demonstrate normal operation and abnormal operation of the tool and will vary depending on the complexity of the tool, the purpose of the tool, and how the tool is used. This verification data may be packaged in any document deemed acceptable by the applicant.

(f) Other tool qualification development data, such as design, code, test cases and procedures, etc. should be available for FAA review.

(3) The ACO engineer and/or DER (if authorized) should strive to use the document format and media used by the applicant for their own purposes. Any repackaging for submittal to the FAA should be undertaken only when the FAA is unable to review the data in any manner proposed by the applicant or the applicant is unable to meet the data retention provisions of the Federal Aviation Regulations.

d. Guidelines for evaluating acceptability of Tool Operational Requirements data: Tool Operational Requirements for any tool that requires qualification should be completed and made available for FAA review. A complete set of operational requirements is necessary to communicate to both the user and the reviewer what the tool does, how it is used, and the environment in which it performs. The Tool Operational Requirements must identify all functional and technical features of the tool and the environment in which it is installed (reference DO-178B, Section 12.2.3.2). The information required is different depending on the type of tool:

(1) For a verification tool, the Tool Operational Requirements should provide at least the following information:

(a) The tool's functionality in terms of specific verifiable requirements that are verified as part of the tool's qualification testing.

(b) A definition of the tool's operational environment, including operating system and any other considerations (e.g., an analysis of what tools will not do and what is required to cover that shortage (e.g., extensions to checklists, test cases) and any specialized hardware requirements (e.g., processors, special test equipment, or interfaces)).

(c) Any other information necessary for the tool's installation or operation (e.g., User's Manual) should be included in the Tool Operational Requirements.

(2) A development tool needs to include all the information listed above for verification tools but should also include at least the following:

(a) Software development processes performed by the tool.

(b) Expected response under abnormal operating conditions.

NOTE: In some cases the User's Manual or other supplier's documentation may contain the needed information. Where additional information is included over and above the required information, the required information should be clearly identified. In the case where there is insufficient information from the tool supplier, the applicant should provide the missing information.

e. Guidelines on acceptable verification of the Tool Operational Requirements: Development and verification tools require verification of the Tool Operational Requirements. For verification tools, only verification over the normal operating conditions is required; whereas for development tools, verification over the abnormal operating conditions is also required. DO-178B Sections 6.4.2.1 and 6.4.2.2 describe verification for normal and abnormal conditions and will not be covered in this notice. However, since the operational requirements may contain additional information not directly related to the verification activity (e.g., the appearance of menus, dialog boxes, configuration), additional guidance is needed to reduce unnecessary verification for verification tools. For verification tools only, those portions of the operational requirements that are used directly in the setting up, conducting, monitoring, and reporting of verification need to be verified as part of tool qualification. The applicant should ensure that those features/portions of the verification tool that are not used have no adverse impact on those features/portions that are being used. If additional features are used at a later time, then additional verification will be required.

f. Guidelines on the interpretation of the determinism of tools:

(1) Although only deterministic tools can be qualified, the interpretation of determinism is often too restrictive. For example, some tools have graphical user interfaces that allow the user to interact in a diagrammatic fashion. Underlying these tools are data tables that capture the intended meaning of those diagrams. Often, however, the output from these tools is at least partially driven by the physical ordering of the entries in these data tables, and the ordering of the data table entries is not under the control of the tool user. It is possible to interpret the output of

this kind of tool as being non-deterministic in the sense that apparently identical diagrammatic input could result in cosmetically (i.e., not functionally significant) different output from the tool. For example, a tool that generates compilable source code from flow chart diagrams might output the alternatives in a switch/case style construct in any one of many possible orders. Such a tool would not be allowed to be qualified under this interpretation of determinism.

(2) What is important is the ability to establish correctness of the output from the tool, not that the same apparent input necessarily leads to exactly the same output. If it can be shown that all possible variations of the output from some given input are correct under any appropriate verification of that output, then the tool should be considered deterministic for the purposes of tool qualification. This results in a bounded problem.

(3) This interpretation of determinism should apply to all tools whose output may vary beyond the control of the user, but where that variation does not adversely affect the intended use (e.g., the functionality) of the output and the case for the correctness of the output is presented. However, this interpretation of determinism does not apply to tools that have an effect on the final executable image embedded into the airborne system. The generation of the final executable image should be totally deterministic.

g. Guidelines for qualifying combined development and verification tools:

(1) The guidelines in this section apply only to tools which provide combined development and verification functions where the output of both the development and the verification functions are being used to eliminate, reduce, or automate processes of DO-178B. Combined tools that are used to eliminate, reduce, or automate only development objective(s) or only verification objective(s) should be qualified as such irrespective of the other capabilities present in that tool.

(2) Qualification of combined tools (when both the development and verification functions are being used to meet or replace objectives of DO-178B) should be performed to the guidance equivalent to the airborne software level ***unless protection/partitioning between the two functions can be demonstrated.*** Acceptable evidence of this protection/partitioning would be to show that the output of one function of the tool has no effect on the output of the other function of the tool (i.e., the tool capabilities are functionally isolated).

(3) When protection/partitioning between the development and verification functions is shown, the protected/partitioned functions may be qualified as if they were separate development and verification tools (i.e., the verification functions may be qualified to the criteria for verification tools).

h. Guidelines on configuration management of qualified tools: In order to receive credit (i.e., meet or replace DO-178B objectives) for the use of qualified tools, those tools must be kept under configuration management. Not all of the requirements for configuration management of tools are contained in DO-178B Section 12.2. Section 12.2.3.b of DO-178B specifies the control

categories for development and verification tool qualification data. DO-178B Section 7.2.9.b contains the requirement that software configuration management be applied to qualified tools.

i. Guidelines on verifying changes to previously qualified tools: A software change impact analysis should be conducted on all changes to tools that have been previously qualified. The analysis should be thorough enough to assess the impact of the tool change on the product, as well as other tools under the influence of the change. A regression analysis may form part of the change impact analysis.

j. Guidelines on DER approval of tool qualification data: If the ACO engineer has delegated compliance findings for tool qualification data, DERs may approve the tool qualification data which complies with the guidance of DO-178B, Section 12.2. However, approval of alternative methods and the resultant data should be retained by the ACO engineer.

7. CONCLUSION. The information and procedures described in this notice constitute a means to more consistently interpret the guidelines for tools qualified in accordance with the provisions of DO-178B, Section 12.2. This notice does not replace or supersede AC 20-115B or DO-178B.

James C. Jones
Manager, Aircraft Engineering Division
Aircraft Certification Service